Havells India

Risk Management, Risk Assessment and Recovery Strategy Procedure

Version 1.0

Document Statistics

S. No.	Type of Information	Document Data
1.	Document Title	Havells India Risk Management Policy
2.	Document Code	HRMP
3.	Date of Release	20th Feb 2023
4.	Document Superseded	
5.	Document	Mr. Pramod Mundra and Mr. Ramanand Jha
6.	Document Owner	Information Security Head
7.	Documents Author(s)	Mr. Sanjay Roongta and Mr. Neeraj Nagpal

Document Approvers

S. No.	Approver	Approver Designation	Approver Contact
1.	Pramod Mundra	Chief Information Officer (CIO)	Pramod.Mundra@havells.com
2.	Ramanand Jha	Information Security Head (ISH)	ramanand.jha@havells.com

Document Change Approvals

Version No.	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	18th Feb 2022
1.0	NA	No change	17th Feb 2023

Document Scope

This document shall be applicable to the IT department and the employees/third parties referred henceforth shall include the staff working with IT department and/or handling, processing, and managing information/information assets of Havells.

Document Distribution

The Information Security Head (ISH) shall distribute this policy to all employees working with IT department and/or handling, processing, and managing information/information assets of Havells by uploading it on the intranet/by sharing it via email/as appropriate.

Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

Table of Contents

1. Purpose

The purpose of this policy is to define how information security risks that could impact the confidentiality, integrity, availability, communication security and privacy of Havells' business process, Information and non-information assets are managed. Risk management is an on-going and re-iterative process that is to be conducted within each Business / Function of Havells.

This policy defines the methodology followed by Havells for conducting risk assessment and formulating the risk treatment plan. It also documents the level of risk deemed acceptable by the Havells' management.

1.1 Scope

This policy (along with Company ERM Policy) shall be applicable to the IT department and the employees/third party who deal with Havells' IT and/or handle, process or manage information/information assets of Havells.

1.2 Responsibility

It is the responsibility of the IT team and respective or concerned business/functional team to implement and maintain the guidelines as defined in the policy.

1.3 Enforcement

All Employees and/or third party, who deal with Havells' IT and/or handle, process or manage information/information assets of Havells, must comply with this policy. All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

a) Non-compliance with this policy shall be dealt with in accordance with the approved management process.

b) Employees and third parties who breach this policy shall be subject to disciplinary action.

Requests for deviations from this policy must be documented and managed using the approved process. Any requests for deviations from this policy must be approved in accordance with the Security Exception Management Policy.

1.4 Authority

The Chief Information Officer (CIO) and Information Security Head (ISH) responsible to enforce this policy and mandate processes to monitor and ensure compliance to this policy.

2. Risk Assessment Procedure

The risk assessment procedure defines a structured approach to perform risk assessment of critical business enablers and assets and business processes of Havells.

Risk Assessment shall be performed on an annual or semi-annual basis or as and when required as per major organizational changes which may include changes in internal/external interested parties, addition/ modification of processes, assets, technical risk evaluation, and when significant changes occur (i.e., adoption of new technology, changes in business, introduction/ amendment in legal or regulatory requirements or when any major information security breach is reported). The details of various risk assessment are given in subsequent sections:

2.1 Process Risk Assessment

Process risk assessment shall address all the risks associated with ISMS at the process level covering key enablers such as information, business process (head office), technology, and people which are essential for smooth functioning of the process. Further, the technology enabler covers key technology asset such as application, IT infrastructure, etc.

2.1.1 Identification of Critical Process

This stage involves listing down all the processes specific to their respective functions. For each process, four kinds of impacts (Financial, Reputational, Legal & Regulatory, Operational) are:

identified across five key risk domains (Confidentiality, Data Integrity, Communication Security, Availability, Privacy) on scale of 1 to 5.

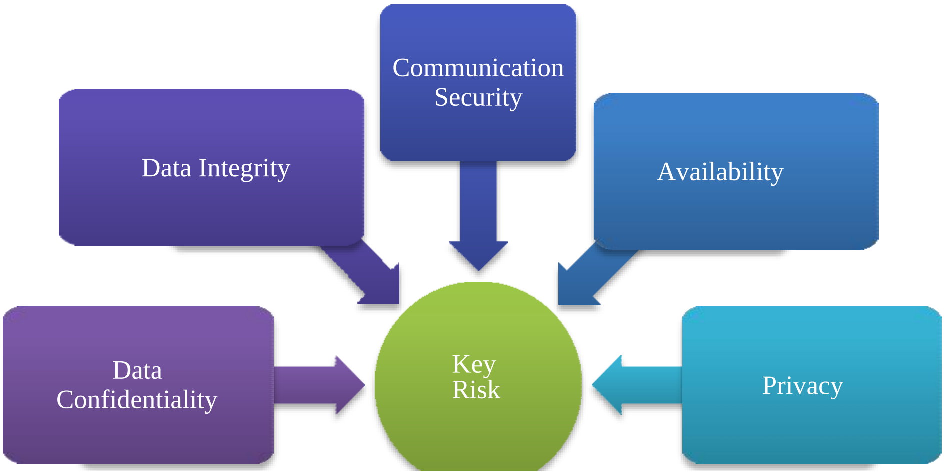


Figure 1: Key Risk

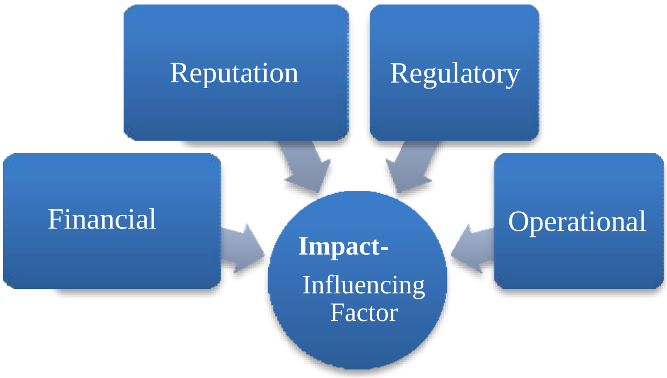


Figure 2: Impact Influencing Factors

Below table shall be considered for determining the impact rating across each IT domain

Type	Score	Financial Impact	Brand Impact	Legal, Regulatory and Contractual Impact	Operational Impact
High	5	Possible revenue impact greater than 5%	Negative impact is national or global and is widely publicized, resulting in negative brand image	Very high penalties, revocation of Licenses etc Severe regulatory scrutiny & litigation & criminal action against senior management	Major effects (more than 10% of the production affected) upon product quality, financial result, production pace and/or delivery time
	4	Possible revenue impact greater than 3% and <=5%	Significant national and Limited international media coverage involves senior executive. Unauthentic information (mix of facts and fiction or unconfirmed fact which has escaped control) is made public	Penalties due to non-Conformance to regulatory/legal/ contractual compliance Multiple scrutiny & litigation	Major effects (6-10% of the Production affected) upon product quality, financial result, production pace and/or delivery time

Type	Score	Financial Impact	Brand Impact	Legal, Regulatory and Contractual Impact	Operational Impact
			over media channels		
Moderate	3	Possible revenue impact greater Than 1 % and <=3%	Unverified and unconfirmed information about the disruption has found its way into local circulation. However, the information is limited to word of mouth and is not made public	Lapse of legal & regulatory obligations, and possibility of penalties/ show cause notice Major scrutiny & litigation	Affects the operations/productions negatively but not severely (5% of the production affected)
Low	2	<=1%	Limited local media coverage The damage on brand due to disruptive incident is reversible.	Minor legal & regulatory obligations, however no penalties/ show cause notice Minor prosecution / litigation	Affects the operations/productions negatively but not severely (2-4% of the production affected)
	1	No revenue impact	No media coverage No reputation impacts. No impact on brand.	No legal/regulatory implications	No or very small effect on the operations/productions (0-1% of the productions affected)

Impact scoring in line with the enterprise risk management framework is depicted in the table below:

Type	Impact Score
High - 3	5
	4
Moderate - 2	3
Low - 1	2
	1

Post identification of impacts, domain impact is calculated across each IT domain for the process.

Domain Impact = Average (Financial, Reputational, Legal and Regulatory, Operational Impact)

The process, the domain impact of which is '3' or greater than 3 (for any one of the domains) shall only be considered for process risk assessment.

2.1.2 Identification of Enablers

Process dashboard shall be created for each process that has been considered for process risk assessment. Enablers across five enabler categories shall be identified by the functional owner for each process

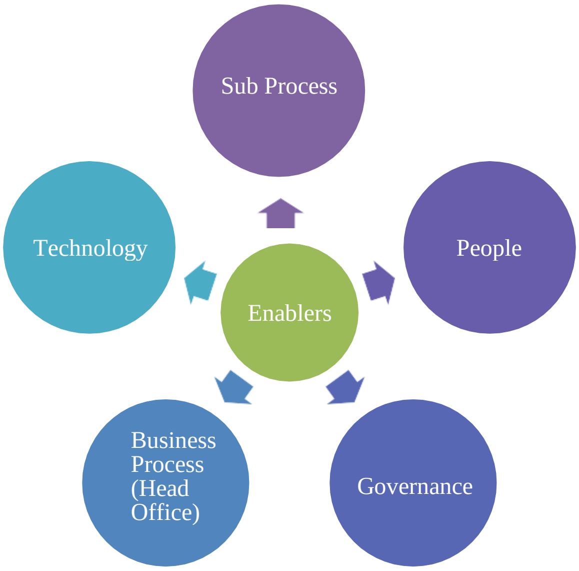


Figure 3: Key Process Enablers

2.1.3 Identification of applicable Threats & Controls

Identification of risk and assessment of controls shall be performed for each process across only those domains whose domain impact is 3 or greater than 3. Threats and corresponding controls shall be identified for the process across applicable domains from the threat and controls masters.

2.1.4 Identification of Likelihood

It defines the probability of occurrence or past known precedence of identified threat. The likelihood- "Likelihood Value" is expressed on a scale of 1-5 as per definitions below:

Type	Likelihood
5 - Almost Certain	Incident occurred in last 1 year or multiple incidents in last 2 years OR Expected to occur in most circumstances
4 – Likely	Incident occurred in last 2 years or multiple incidents in last 3 years OR Will probably occur in most circumstances

Type	Likelihood
3 – Possible	Incident occurred in last 3 years or multiple incidents in last 5 years OR Might occur at some time
2 – Unlikely	Incident occurred in last 5 years or multiple incidents in last 7 years OR Could occur at some time
1 - Rare	No Incident occurred in last 5 years OR May only occur in exceptional circumstances.

In addition, parameters like geographical location, surrounding, political, environmental factors will be considered while deciding the likelihood of any risk.

2.1.5 Control Rating Computation

2.1.5.1 Category & Type of Control

All the applicable controls in the control database are categorized basis five identified enablers. Each control is mapped to one enabler in the control database. Further, controls are segregated basis preventive, detective & corrective control types.

Post identification of the control category, controls are mapped to the applicable threats, basis the threat vulnerabilities.

2.1.5.2 Enabler Control Effectiveness Score

After mapping of threats, controls & enablers, enabler assessment is created basis the applicable threat across the domains identified for the process. For each threat likelihood is identified basis the geographical location, surrounding, political, environmental factors etc. Further, a constant impact rating = 1 (for computation purpose only) is considered for each of the threats identified in the enable assessment.

Control Rating: Control rating depicting the implementation status of the control (as per the below table) is identified by the assessor for each control in the enabler assessment.

Control Rating	Definition
1	Non-existent or has major deficiencies and do not operate as intended.
2	Limited, high level of risk remains, significant deficiencies.
3	Controls in place with few deficiencies in terms of medium risk issues.
4	Designed and operating, with few deficiencies in terms of low risk issues.
5	Designed and operating, with no deficiencies.

The control ratings are used to identify the revised likelihood score and revised impact score in order to calculate the residual risk score for the corresponding threats as per the table below:

Average Preventive Control Score (for each threat)	Revised Threat Likelihood
0 to 1	Like * 1
1 to 2	Like * 0.8

2 to 3	Like * 0.5
3 to 4	Like * 0.3
4 to 5	Like * 0.1

Average Detective/Corrective Control Score (for each threat)	Revised Threat Impact
0 to 1	Like*1
1 to 2	Like*0.8
2 to 3	Like*0.5
3 to 4	Like*0.3
4 to 5	Like*0.1

Threat Residual Risk Score = Revised (Likelihood * Impact)

Enabler Residual Risk Score = Average (Threat Residual Risk Score)

2.1.5.3 Domain Residual Base Risk

After calculation of each residual risk score for each enabler across the process, the domain residual base risk is computed using the below formula:

Domain Residual Base Risk = Average (Enabler Residual Risk Score)

2.1.6 Risk Computation

2.1.6.1 Calculate Residual Risk Value

After calculation of domain residual base risk for each applicable domain of the process, the domain impact score is used to calculate the domain residual risk value of each applicable domain:

Residual Risk Value = (Domain Impact * Domain Residual Base Risk)

2.1.6.2 Risk acceptance/ Treatment/ Transfer level

The possible values of existing risk post calculation of residual risk are:

Residual Risk Score	Risk Description	Management action
1-4	Low Risk	Accept risk - No action required
5-10	Moderate Risk	Accept risk- Feasibility analysis
11 - 25	High Risk	Treat/ transfer risk

If the management wants to accept or transfer any risk as per the results obtained from the risk assessment, proper justification has to be provided. Risk shall be accepted for a number of reasons including but not limited to:

a) The potential impact is low, and cost of further protection against risk is not worthwhile in business terms;

b) The likelihood of an incident is low, and the cost of further protection against the risk is not worthwhile in business terms; and

c) The risk cannot be avoided, transferred, or mitigated any further within acceptable costs to the businesses.

2.1.6.3 Risk Transfer

Risk transfer involves a decision to share certain risks with external/ internal parties. Risk transfer can create new risks or modify existing, identified risks. Therefore, additional risk assessment followed by risk treatment may be necessary. Transfer can be done by insurance that shall support the consequences, or by sub-contracting a partner whose role shall be to monitor the information system and take immediate actions to stop an attack before it makes a defined level of damage.

2.1.6.4 Risk Treatment

Risk Treatment Plan (hereafter referred to as RTP) involves prioritizing, evaluating, and implementing appropriate controls as per the risk computation. A treatment plan shall be prepared for each identified risk as per the risk assessment performed.

To facilitate the implementation of the risk treatment plan, an action plan shall be prepared, and responsibility shall be assigned for implementing the recommended controls. The plan shall also clearly highlight the expected and actual closure date of implementation.

2.1.6.5 Closure Responsibility, Target Completion Date and Status

Details (Name, role, etc.) of the person responsible for the closure of the risk identified will be captured along with the target date of completion for the same and the status of risk closure.

Once recommended controls have been identified, residual risk value shall be computed with the same approach as followed for “Risk Rating” to identify if the residual risk value is at acceptable level or additional controls need to be defined to mitigating the risks.

2.1.6.6 Management approval

It is the responsibility of respective department head to present risk treatment plan to the management for approval, and regularly update on the progress of RTP.

2.2 Site Risk Assessment

Site risk assessment shall be conducted for **Havells’ head office**.

2.2.1 Site Risk Assessment Steps

2.2.1.1 Step 1 : Identify the site category

Category of site should be identified

2.2.1.2 Step 2 : Perform the site Survey

The administration team shall be given responsibility to conduct the on-ground assessment.

2.2.1.3 Step 3 : Perform the Risk Assessment

Administration team shall use the Site Gap Assessment checklist which is outlined on the basis of compliance to Havells Physical Security Management Policy. Administration team shall use the checklist specific to their site category to perform site risk assessment for the identified critical facility. The domains considered in the site gap assessment checklist are as follows, but not limited to:

a) Facts about head office ;
b) Fire safety;
c) Electrical and mechanical systems;
d) Building management system;
e) Physical security; and
f) Site administration and management

The observations and findings should be identified during the survey as per the risk assessment checklist. Also, these areas will be considered during the gap assessment.

a) Legal and regulatory requirements/certificates;
b) Insurance considerations; and
c) IT considerations

The supporting documents and evidence for the observations in the gap assessment checklist should be verified and documented with the gap assessment report for the facility.

2.2.1.4 Step 4 : Management response on site risk assessment report

a) Basis the compliance or non-compliance to Havells' Physical Security Management Policy, administration team shall prepare a summary report;
b) Administration team shall document response against the gaps and recommendations to mitigate the gaps for the top threats identified for the Head Office;
c) Havells' respective IT Lead h shall communicate the findings (forward the report) to ISH/CIO for reference;
d) IT Lead and administration team shall formulate an implementation plan for the observations in the gap assessment report along with the timelines and responsibilities and ISH/CIO/ Administration team head shall approve the implementation plan.

2.2.2 Risk Treatment Plan

The management shall consider the following four options to treat the gaps highlighted in the risk treatment plan:

a) Accept;
b) Treat; and
c) Transfer.

Risk Category	Management Recommendation
High	Risk should be treated immediately
Medium	Risk treatment plan should be developed, and controls implemented after High risk category controls have been implemented
Low	Management should consider the treatment in future, if not immediately

2.2.3 Risk Acceptance

Any exception to Havells Physical Security and Management Policy will require an exception. It should be signed off by the management.

(Refer: Havells Physical Security Management Policy, Security Exception Management Policy)

2.3 Interested parties – Issues

Risks and opportunities are determined against each identified interested parties and action plan is determined. The issues of interested parties are identified and mapped to relevant risks under the Process Risk Assessment [Refer Section 2.1: Process Risk Assessment]. Mapping has been done to the applicable risks deriving the issues against these interested parties post considering the residual risk value of the identified risk.

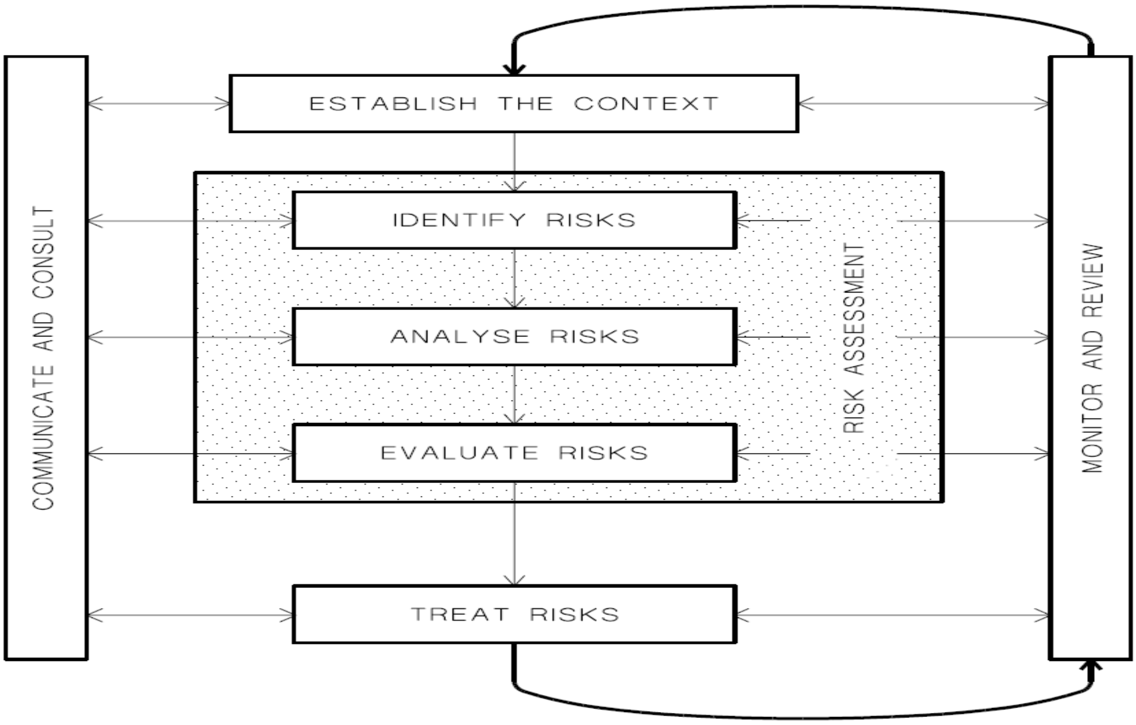
2.4 Recovery Strategy Procedure

The recovery strategies formulation for Havells' critical processes is discussed in section 2.1. All recovery strategies should be formulated keeping in mind the six R – Reduce, Respond, Recover, Resume, Restore and Return that is, being able to:

a) Reduce an impact of a BC/ DR event
b) Respond to a BC/DR event
c) Recover from a BC/DR event
d) Resume critical business processes after a BC/DR event
e) Restore the primary site after a BC/DR event
f) Return to normal operations

2.5 Risk Management Methodology

The risk management framework is based on the traditional standards-based risk management framework as described in ISO/IEC 27005 and ISO/IEC 31000 and shown below:



2.5.1 Establish the context

The objectives and the factors that may influence Havells' information security requirement as well as information security risks must be identified prior to assessing risks.

2.5.2 Identify Risks

Information security risk impacting the confidentiality, integrity, availability, communication security and privacy of Havells Information Asset must be identified. These include but are not limited to IT security risks.

Risk identification can come from a variety of sources such as internal and external audit, regulatory reviews, self-assessments, etc. Risk identification is to be an ongoing and continual process across Havells.

2.5.3 Analyze and Evaluate risks

a) Risk identified shall be analyzed to identify existing controls within the environment and evaluates the effectiveness of controls in lowering the identified risk;

b) The output of the risk identification shall contain a description of the risks and of potential consequences as well as current (existing) and a residual (post mitigation) risk rating for each risk based on a combination of the impact of an event occurring and the likelihood of the event occurring;

c) The risk evaluation shall determine the overall risk rating and the severity of the risk;

d) Risk evaluation must leverage the risk metric define in this standard to ensure a consistent understanding and interpretation of risks within Havells;

e) Each Risk must be assigned to, and accepted by, a Risk Owner and is the responsibility of that Risk Owner.

2.5.4 Treat and control risks

a) Risk Owners must formally either Treat, Accept, Transfer or Terminate their risks;

b) In order to manage their risks, and in accordance with the risk appetite defined in this policy, risk owners may:

   i. Terminate a risk - avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

   ii. Transfer a risk - sharing the risk with another party or parties through contracts, insurance or risk financing;

   iii. Treat a risk - reducing the risk by removing the risk source to reduce the likelihood and/or consequences;

   iv. Accept a risk - retaining the risk following an informed decision and evaluating the anticipated decisions;

c) When treating a risk, a risk treatment plan (which can consist in one or more actions) must be formally developed to an acceptable level.

2.5.5 Risk Treatment Plan

Risk Treatment Plan involves prioritizing, evaluating and implementing appropriate controls as per the risk computation. A treatment plan shall be prepared for each identified risk as per the risk assessment performed.

To facilitate the implementation of the risk treatment plan, an action plan shall be prepared, and responsibility shall be assigned for implementing the recommended controls. The plan shall also clearly highlight the expected and actual closure date of implementation.

2.5.5.1 Monitor and review

a) Risks and treatment plans shall be continually monitored and reviewed to ensure risks are being managed effectively and to ensure that risk management processes are operating effectively;

b) Monitoring activities shall be periodically conducted to ensure that risk treatments have been implemented as planned.

2.5.5.2 Communicate and Consult

a) All departmental heads must establish the Information Security Council (ISC) representing functional areas within their business entity;

b) The ISC must establish an enterprise-level Information Security Team representing business function.

2.6 Havells Risk Metrics & Appetite

2.6.1 Impact

Type	Score	Financial Impact	Brand Impact	Legal, Regulatory and Contractual Impact	Operational Impact
High	5	Possible revenue impact greater than 5%	Negative impact is national or global and is widely publicized, resulting in negative brand image	Very high penalties, revocation of Licenses etc Severe regulatory scrutiny & litigation & criminal action against senior management	Major effects (more than 10% of the production affected) upon product quality, financial result, production pace and/or delivery time
		Possible revenue impact	Significant national and Limited	Penalties due to non-Conformance to	Major effects (6-10% of the Production

Type	Score	Financial Impact	Brand Impact	Legal, Regulatory and Contractual Impact	Operational Impact
	4	greater than 3% and <=5%	international media coverage involves senior executive. Unauthentic information (mix of facts and fiction or unconfirmed fact which has escaped control) is made public over media channels	regulatory/legal/ contractual compliance Multiple scrutiny & litigation	affected) upon product quality, financial result, production pace and/or delivery time
Moderate	3	Possible revenue impact greater Than 1 % and <=3%	Unverified and unconfirmed information about the disruption has found its way into local circulation. However, the information is limited to word of mouth and is not made public	Lapse of legal & regulatory obligations, and possibility of penalties/ show cause notice Major scrutiny & litigation	Affects the operations/productions negatively but not severely (5% of the production affected)
Low	2	<=1%	Limited local media coverage The damage on brand due to disruptive incident is reversible.	Minor legal & regulatory obligations, however no penalties/ show cause notice Minor prosecution / litigation	Affects the operations/productions negatively but not severely (2-4% of the production affected)

Type	Score	Financial Impact	Brand Impact	Legal, Regulatory and Contractual Impact	Operational Impact
	1	No revenue impact	No media coverage No reputation impacts. No impact on brand.	No legal/regulatory implications	No or very small effect on the operations/productions (0-1% of the productions affected)

2.6.2 Likelihood

Type	Likelihood
5 - Almost Certain	Incident occurred in last 1 year or multiple incidents in last 2 years OR Expected to occur in most circumstances
4 – Likely	Incident occurred in last 2 years or multiple incidents in last 3 years OR Will probably occur in most circumstances
3 – Possible	Incident occurred in last 3 years or multiple incidents in last 5 years OR Might occur at some time
2 – Unlikely	Incident occurred in last 5 years or multiple incidents in last 7 years OR Could occur at some time
1 – Rare	No Incident occurred in last 5 years OR May only occur in exceptional circumstances.

2.6.3 Risk Level

		Consequence				
		Negligible (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Likelihood	Almost Certain (5)	Low (5)	Medium (10)	High (15)	Very High (20)	Very High (25)
	Likely (4)	Low (4)	Medium (8)	Medium (12)	High (16)	Very High (20)
	Possible (3)	Low (3)	Low (6)	Medium (9)	High (12)	High (15)
	Unlikely (2)	Low (2)	Low (4)	Low (6)	Medium (8)	High (10)

	Rare (1)	Low (1)	Low (2)	Low (3)	Medium (4)	Medium (5)

2.6.4 Havells Action and Approval (Risk Appetite)

Type (in line with enterprise risk management framework)	**Risk Rating**	**Response/Action**
3	High	High risks are unacceptable or intolerable and must be avoided except in extraordinary circumstances. An alternative solution must be found, and all necessary steps must be taken to reduce the risk below this level without delay.
2	Medium	Action plan shall be defined against medium risks and shall be mitigated as per the defined timelines
1	Low	Low risks are tolerable and acceptable if it is not reasonably practicable to further reduce the risk.